Publication No. --- JP-Sho63-279289
Publication Date --- November 16, 1988
Title --- ENCRYPTION PROCESSING METHOD
Application No. --- JP-Sho62-114244
Filing Date --- May 11, 1987
Applicant --- NEC Corporation
Inventor --- Tatsuo TANIGAMI

ABSTRACT

This document discloses an encryption processing method suitable for an information processing device, wherein an encryption key includes information about the number of encryption processes, and the information is decoded and accordingly the number is obtained from the encryption key, and then a plurality of encryption processing blocks corresponding to the number of encryption processes are selected, and thus the encryption processes are performed by the plurality of encryption processing blocks.

According to the above technique, when the number of encryption processes is set to be large, its cryptographic strength becomes high even though its processing speed becomes slow. This is suitable for encrypting a small amount of particularly important data.

On the other hand, when the number of encryption processes is set to be small, the processing speed becomes fast even though the cryptographic strength becomes low. This is suitable for encrypting a relatively large amount of data which does not require a long secrecy period.

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭63－279289

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和63年(1988)11月16日
G 09 C 1/00		7368－5B	

審査請求　未請求　発明の数 1　（全4頁）

⑤4発明の名称　暗号処理方式

⑳特　願　昭62－114244
㉒出　願　昭62(1987)5月11日

⑦2発明者　谷上　達郎　東京都港区芝5丁目33番1号　日本電気株式会社内
⑦1出願人　日本電気株式会社　東京都港区芝5丁目33番1号
⑦4代理人　弁理士　井出　直孝

明　細　書

1. 発明の名称

暗号処理方式

2. 特許請求の範囲

(1) 暗号用キーを入力して複数個のキーを作成し暗号化時と復号化時とでは順番を逆にして出力するキー供給回路と、

この複数個のキーをそれぞれ入力し暗号化または復号化するデータについて処理を順番に行う複数個の暗号処理ブロックと

を備えた暗号処理方式において、

上記暗号用キーは、暗号処理を行う回数を示す情報を含み、

この情報を解読して処理回数を出力する処理回数解読回路と、

上記処理回数に基づいて暗号処理を行うように上記複数個の暗号処理ブロックを選択する処理回数切換手段と

を備えたことを特徴とする暗号処理方式。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明は、情報処理装置に適する暗号処理方式に関する。特に、暗号化処理回数を可変にして柔軟な暗号化を行えるようにした慣用系暗号器の可変型の暗号処理方式に関する。

〔概　要〕

本発明は情報処理装置に適する暗号処理方式において、

暗号用キーに暗号処理の回数の情報を含ませ、この情報を解読し解読した処理回数に対応する暗号処理ブロックを選択することにより、

情報処理装置の扱うデータ量と機密性とに見合った暗号強度および暗号処理性能を柔軟に設定できるようにしたものである。

〔従来の技術〕

従来、暗号処理方式は、n個の暗号処理ブロックでn回の暗号化処理を行うことによってその暗

号強度を保つようにされていた。このような従来の暗号処理方式としては米国のエフ・アイ・ピー・エス（ＦＩＰＳ，Federal Information Processing Standards)の制定したデータ暗号規格(Date Encryption Standard 方式、以下、ＤＥＳ方式と云う。）がある（ＦＩＰＳ Publicatoin 46)。

このＤＥＳについては、岩波書店発行　岩波講座　情報科学－４　情報と符号の理論　１９８５年　頁 223～227　宮川洋他に概要が記載されている。

〔発明が解決しようとする問題点〕

しかし、このような従来の暗号処理方式では、暗号論理自体が公開され、大規模集積回路化され市販される等暗号の普及に有利であるが、暗号の強度を保つことに専念するあまり暗号化処理を組込んだ情報処理装置では以下に示すような欠点があった。すなわち、

①　大量のデータを処理する必要のあるデータ処理、たとえば磁気テープファイルを用いたデータ交換などに適用すると多段式の暗号処理（ＤＥＳ方式では16段）では暗号化に費す時間が多くかかるために全体の処理時間が長くなりすぎる、

②　情報の持つ秘匿価値が短期間に減少するような情報（たとえば新聞など発表する前の企業の決算報告等）を同一情報処理装置で暗号化する場合でも重要機密に対すると同様に解読に何年もかかるような暗号強度を保つようにしか暗号化できないために、不要な暗号化処理時間を費すことになる、

などの欠点があった。

本発明は上記の欠点を解決するもので、情報処理装置の扱うデータ量と機密性とに見合った暗号強度および暗号化処理速度を柔軟に設定できる暗号処理方式を提供することを目的とする。

〔問題点を解決するための手段〕

本発明は、暗号用キーを入力して複数個のキーを作成し暗号化時と復号化時とでは順番を逆にして出力するキー供給回路と、この複数個のキーをそれぞれ入力し暗号化または復号化するデータについて処理を順番に行う複数個の暗号処理ブロックとを備えた暗号処理方式において、上記暗号用キーは、暗号処理を行う回数を示す情報を含み、この情報を解読して処理回数を出力する処理回数解読回路と、上記処理回数に基づいて暗号処理を行うように上記複数個の暗号処理ブロックを選択する処理回数切換手段とを備えたことを特徴とする。

〔作　用〕

暗号用キーに含まれた暗号処理を行う回数を示す情報を処理回数解読回路で解読して処理回数を出力する。処理回数切換手段でこの処理回数に基づいて暗号処理を行う暗号処理ブロックを選択する。以上の動作により情報処理装置の扱うデータ量と機密性とに見合った暗号強度および暗号処理性能を柔軟に設定できる。

〔実施例〕

本発明の実施例について図面を参照して説明する。図は本発明一実施例暗号処理装置のブロック構成図である。図において、暗号処理装置は、図外から暗号用キーが入力する入力端子Ａと、入力端子Ａから暗号用キーを入力し所定の規則に従ってｎ個の異なるキーＫ１～Ｋｎを作成し暗号化時と復号化時とでは順序を逆にして出力するキー供給回路１と、キー供給回路１からキーＫ１～Ｋｎを入力して暗号化または復号化の処理を行う縦続接続された暗号処理ブロック２１～２ｎとを備える。

また、暗号処理装置は、図外から入力する暗号用キーは暗号化または復号化する処理回数を示す情報が含まれ、この情報を解読する処理回数解読回路３と、図外から平文または暗号文を入力する入力端子Ｂと、入力端子Ｂから平文または暗号文を入力し、処理回数解読回路３から暗号化時には処理回数ｘまだは復号化時には復号化であることを入力して内部スイッチを切り換える（復号時は端子ａ）暗号処理回数切換器４と、暗号処理回数切換器４の出力を処理回数ｘの暗号処理ブロック２を経由するように、またたとえば64ビットの出力を32ビットずつに２分して暗号処理ブロック２に与える分割回路５と、暗号処理４から32ビット

ずつに2分された暗号化または復号化処理されたデータを入力し左右入れ換えた後に64ビットに戻す併合回路6と、処理回数解読回路3から暗号化時には暗号化であることまたは復号化時には処理回数xを入力して内部スイッチを切り換えて（暗号時は端子b）併合回路6の出力を入力する復号処理回数切換器7と、復号処理回数切換器7の出力を入力して図外に出力する出力端子Cを備える。

このような構成の暗号処理装置の動作について説明する。図において、まず暗号用キーを決める。次に、この実施例では暗号用キーに暗号化の処理回数の情報を含ませる。すなわち、暗号用キーの作り方はたとえば従来のように乱数を発生させて暗号用キー（たとえばDES方式では56ビット）を得た後にその先頭mビットで処理回数を示すように先頭mビットを変更する公知な方法を用いる。図では、上記暗号用キーの先頭mビットに処理回数を示す方法を用いた場合で説明する。

まず入力端子Aから暗号用キーを入力しまた入力端子Bから平分を入力する。処理回数解読回路3は、暗号用キーの先頭mビットを解読し処理回数xを得た後に、暗号処理回数切換器4に処理回数xを通知する。また復号処理回数切換器7に暗号化であることを通知する。暗号処理回数切換器4は処理回数xに従って内部スイッチを切り換え、平文がx段分のブロックを通過して暗号化されるように回路を持続する。また復号処理回数切換器7は暗号化である旨の指示に従って信号処理ブロック2n出力を得るように回路を接続する。

図では

$x = n - 1$

の場合を示しており、平文はキー供給器1によって得られたキーK_xに従って暗号処理ブロック2_xで暗号化され、次にキーK_xに従って暗号処理ブロックに暗号化され以後同様にキーK_nに従って暗号処理ブロック2_nによって暗号化されて暗号文となり、端子bを経て出力端子Cから出力される。すなわち、平文は暗号用キーの先頭mビットに格納された処理回数xだけ暗号化処理を受ける。

次に、暗号文を平文に戻す復号化処理では、上記暗号化時に与えた暗号用キーと同じものを入力端子Aから入力し、また暗号文を入力端子Bから入力する。処理回数解読回路3は暗号用キーの先頭mビットより処理回数xを得た後に復号処理回数切換器7に処理回数xを通知する。また、暗号処理回数切換器4には復号化であることを通知する。復号処理回数切換器7は処理回数xに従って内部スイッチを切換え、暗号文がx段分の暗号処理ブロック2を通過して復号化されるように、また暗号処理回数切換器4は、復号化である旨の指示に従って暗号処理ブロック2_1に入力を与えるように各々回路を接続する。上述のようにして得た暗号文を復号化する場合には、入力端子Bからの入力は端子aを通って暗号処理ブロック2_1へ流れ、出力端子cへの出力は暗号処理ブロック2_xから流れるように接続される。

暗号文はキー供給器1によって逆順に与えられたキーK_nに従って暗号処理ブロック2_1で復号化され、次にキーK_{n-1}に従って暗号処理ブロック2_2でさらに復号化され、以後同様にキーK_xに従って暗号処理ブロック2_{n-1}で復号化されて平文となり出力端子Cから出力される。すなわち、平文は暗号用キーの先頭mビットに格納された処理回数xだけ復号化処理を受ける。

上述のように、本実施例は暗号処理回数を多くすれば処理性能は遅いが暗号強度は強いものが得られるので特に重要な少量の情報の暗号化に適しており、また暗号処理回数を少なくすれば暗号強度は弱いが処理性能が速いので秘匿期間があまり長くなく大量の情報の暗号化に適した暗号処理を実現することができる。

〔発明の効果〕

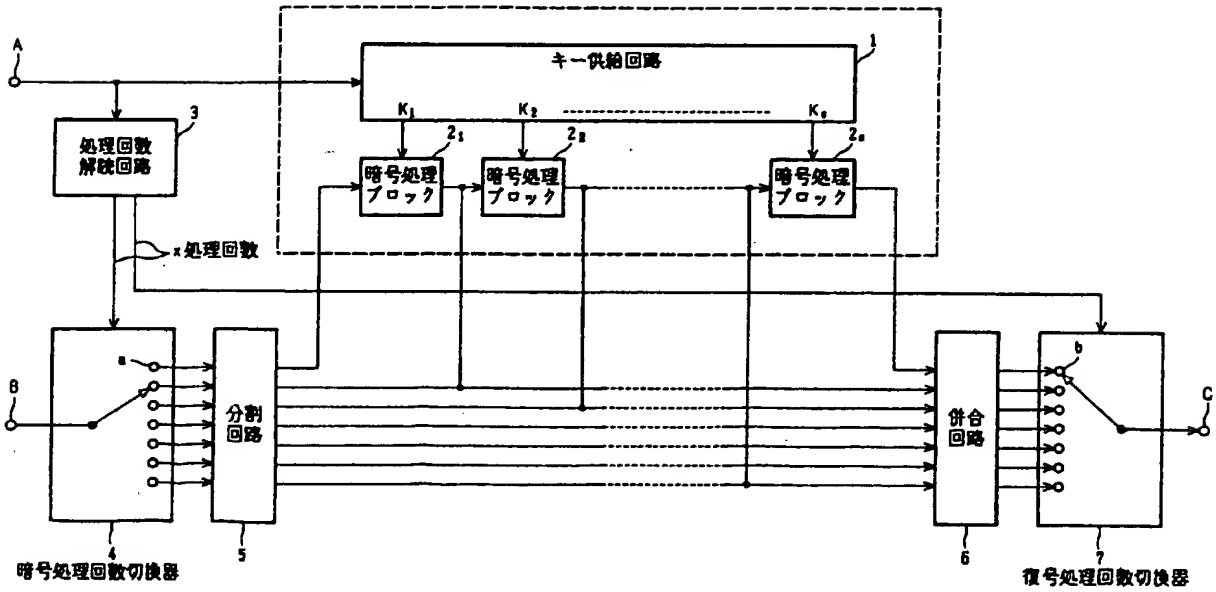
以上説明したように、本発明は、暗号用キーに暗号処理回数の情報を含ませ、この情報を処理回数解読回答で読み取って暗号化処理および復号化処理の回数を制御することにより、情報処理装置が扱うデータの量と機密性とに見合った暗号強度および暗号処理性能を柔軟に設定できる優れた効果がある。

4. 図面の簡単な説明

図は本発明一実施例暗号処理装置のブロック構成図。

1…キー供給回路、2₁～2ₙ…暗号処理ブロック、3…処理回数解読回路、4…暗号処理回数切換器、5…分割回路、6…併合回路、7…復号処理回数切換器、A、B…入力端子、C…出力端子、K₁～Kₙ…キー、a、b…端子、x…処理回数。

特許出願人　日本電気株式会社
代理人　弁理士　井出直孝



実施例